US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary
- December 2010 -

This report summarizes general activity as well as updates made to the National Cyber Alert System in December 2010. It includes current activity updates, technical and non-technical cyber security alerts, cyber security bulletins, and cyber security tips, in addition to other newsworthy events or highlights.

Executive Summary

During December 2010, US-CERT issued sixteen Current Activity entries, one Technical Cyber Security Alert, one Cyber Security Alert, four weekly Cyber Security Bulletins, and one Cyber Security Tip.

Highlights for this month include updates or advisories released by Apple, Microsoft, and OpenSSL; fraud advisories for holiday season consumers; and security practices when using removable media.

Contents

Current Activity

Current Activity entries are high-impact security threats and vulnerabilities presently being reported to US-CERT. The table lists all of the entries posted this month followed by a brief overview of the most significant entries.

Current Activity for December 2010	
December 1	VMware Releases Security Patch for ESX
December 1	Potential WikiLeaks Phishing Scams
December 2	WordPress Releases WordPress 3.0.2
December 2	Internet Systems Consortium BIND Vulnerabilities
December 3	VMware Releases Security Advisory VMSA-2010-0018
December 3	Google Releases Chrome 8.0.552.215
December 8	Apple Releases QuickTime 7.6.9
December 9	WordPress Releases Version 3.0.3
December 9	Microsoft Releases Advance Notification for December Security Bulletin
December 10	Mozilla Releases Firefox 3.6.13

Current Activity for December 2010	
Dec 13	RealNetworks Releases Security Update for RealPlayer
Dec 14	Microsoft Releases December Security Bulletin
Dec 14	Google Releases Chrome 8.0.552.224
Dec 15	RIM Releases Security Advisory for BlackBerry Enterprise Server
Dec 20	Microsoft Releases Blog Entry Regarding Recent Outlook 2007 Update *
Dec 20	Holiday Season Phishing Scams and Malware Campaigns
Dec 22	Microsoft WMI Administrative Tool Active X Control Vulnerability *

- Apple released QuickTime 7.6.9 to address multiple vulnerabilities. Exploitation of these vulnerabilities may allow an attacker to execute arbitrary code, cause a denial-of-service condition, or obtain sensitive information.
- Chrome 8.0.552.215 and 8.0.552.224 addressed vulnerabilities that may allow an attacker to execute arbitrary code, cause a denial-of-service condition, obtain sensitive information or bypass security restrictions.
- Microsoft released its December Security Bulletin and addressed recent issues related to Outlook 2007 in a subsequent blog entry.
  - The Microsoft Security Bulletin for December provided updates to address vulnerabilities in Microsoft Windows, Internet Explorer, Office, SharePoint, and Exchange as a part of the Microsoft Security Bulletin Summary. These vulnerabilities may allow an attacker to execute arbitrary code, operate with elevated privileges, or cause a denial-of-service condition.
  - The Microsoft Outlook product team posted a blog entry to inform users of several issues related to the Outlook 2007 update (KB2412171) released as part of the monthly update. The blog entry indicated that this update has been removed from Microsoft Update. Users who previously applied the update and are experiencing any of the listed issues are encouraged to uninstall the December 2010 update as described in the blog entry.
- Mozilla released Firefox 3.6.13 to address multiple vulnerabilities that may allow an attacker to execute arbitrary code, operate with elevated privileges, spoof the location bar, or operate with elevated privileges. The Mozilla foundation also released Firefox 3.5.16 to address these same vulnerabilities. US-CERT encourages users and administrators to review the Mozilla Foundation Security Advisories released on December 9, 2010 and apply any necessary updates to help mitigate the risks.
- RealNetworks, Inc. released an update for RealPlayer to address multiple vulnerabilities. Exploitation of these vulnerabilities may allow an attacker to execute arbitrary code.

- VMware addressed vulnerabilities with the release of a multiple security patches.
  - VMware released a security patch for ESX to address a vulnerability. Exploitation of this vulnerability may allow a local user to gain additional privileges on the affected system. US-CERT encourages users and administrators to review VMware knowledgebase article 1029397 and apply any necessary updates to help mitigate the risks.
  - VMware released security advisory VMSA-2010-0018 to address multiple vulnerabilities affecting VMware Workstation, Player, Fusion, ESXi, and ESX.
- WordPress released WordPress 3.0.3 to address a vulnerability. Execution of this vulnerability may allow an attacker to operate with elevated privileges. US-CERT encourages users and administrators to review the WordPress Codex document for version 3.0.3 and apply any necessary updates to help mitigate the risks.

Technical Cyber Security Alerts

Technical Cyber Security Alerts are distributed to provide timely information about current security issues, vulnerabilities, and exploits.

Technical Cyber Security Alerts for December 2010	
December 14	TA10-348A Microsoft Updates for Multiple Vulnerabilities

Cyber Security Alerts

Cyber Security Alerts are distributed to provide timely information about current security issues, vulnerabilities, and exploits. They outline the steps and actions that non-technical home and corporate users can take to protect themselves.

Cyber Security Alerts (non-technical) for December 2010	
December 9	SA10-348A Microsoft Updates for Multiple Vulnerabilities

Cyber Security Bulletins

Cyber Security Bulletins are issued weekly and provide a summary of new vulnerabilities recorded by the National Institute of Standards and Technology's (NIST's) National Vulnerability Database (NVD). The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / US-CERT. For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

Security Bulletins for December 2010
SB10-347 Vulnerability Summary for the Week of December 6, 2010
SB10-354 Vulnerability Summary for the Week of December 13, 2010
SB10-361 Vulnerability Summary for the Week of December 20, 2010

A total of 210 vulnerabilities were recorded in the NVD during December 2010.

Cyber Security Tips

Cyber Security Tips are primarily intended for non-technical computer users. The focus of December's tip regarded the popularity of online shopping and the unique risks presented by the Internet.

Cyber Security Tips for December 2010	
December 6	ST07-001 Shopping Safely Online

Security Highlights

Potential WikiLeaks Phishing Scams

In the past, US-CERT has received reports of phishing scams and malware campaigns related to topics that are of high interest to the U.S. Government or news media, such as the WikiLeaks website. Users' systems have been compromised by receiving and accessing phishing e-mails with subject lines that seem relevant to a high-interest subject and appear to originate from a valid sender. US-CERT reminds users to remain vigilant for potential malicious cyber activity seeking to capitalize on interest in WikiLeaks. Users are advised to exercise caution in handling any e-mail with subject line, attachments, or hyperlinks related to WikiLeaks, even if it appears to originate from a trusted source.

Contacting US-CERT

If you would like to contact US-CERT to ask a question, submit an incident, or learn more about cyber security, please use one of the methods listed below. If you would like to provide feedback on this report, or if you have comments or suggestions for future reports, please e-mail info@us-cert.gov.

Web Site Address: http://www.us-cert.gov
E-mail Address: info@us-cert.gov
Phone Number: +1 (888) 282-0870
PGP Key ID: 0x91D70D64
PGP Key Fingerprint: EAAC 46A4 4CEC 8A78 EED2 73F3 E5F3 5D6C 91D7 0D64
PGP Key: https://www.us-cert.gov/pgp/info.asc